AFFIDAVIT

I, Aaron Lindaman, state:

INTRODUCTION AND AGENT BACKGROUND

1. I have been a Special Agent/Criminal Investigator with the United States Department of Homeland Security, Homeland Security Investigations ("HSI") for approximately 14 years. Before that assignment, I was employed as a Border Patrol Agent for approximately 5 years. I am currently assigned to conduct investigations as a Special Agent in the Boston Office of HSI. As a Special Agent, I am authorized as an officer of the United States to conduct investigations and to make arrests for offenses enumerated in Titles 8, 18, and 19 of the United States Code. I have received on-the-job and HSI-sponsored training on these types of investigations. My investigations and training have included the use of surveillance techniques and the execution of search, seizure, and arrest warrants.

2. I am currently investigating KELECHI COLLINS UMEH, also known as "Bishop," also known as "Jacob Emmanuel," also known as "James Emmanuel," also known as "Kelvin Thomas," also known as "Paul Douglas" also known as "Brian Morgan," also known as "John Isiah," for mail, wire, and bank fraud, as well as conspiracy to commit those crimes, in violation of 18 U.S.C. §§ 1341, 1343, 1344 and 1349, respectively; making a false statement to a bank, in violation of 18 U.S.C. § 1014; and money laundering, in violation of 18 U.S.C. §§ 1956 and 1957 (collectively, the "TARGET OFFENSES").

3. I submit this affidavit in support of a criminal complaint charging UMEH with conspiracy to commit bank fraud, in violation of 18 U.S.C. § 1349 and for a warrant to arrest UMEH. As further described below, there is probable cause to believe that beginning no later than 2018 and continuing through at least 2020, UMEH and others known and unknown conspired to

defraud banks by opening bank accounts using aliases and fake passports and by using those accounts to receive and launder the proceeds of romance, advance fee, and business email compromise ("BEC") schemes.

4. I also submit this affidavit in support of an application for a warrant to search UMEH's person (the "TARGET PREMISES"), as described in Attachment A to the proposed warrant, because there is probable cause to believe that it contains evidence, fruits, and instrumentalities of the TARGET OFFENSES, as described in Attachment B to the proposed warrant.

5. The facts in this affidavit come from my personal observations and review of records, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is probable cause for the requested complaint and warrant and does not set forth all of my knowledge about this matter.

PROBABLE CAUSE TO BELIEVE THAT A FEDERAL CRIME WAS COMMITTED

6. A "romance scam" is a type of fraud that is enabled by the creation of fictitious profiles on online dating or social websites. "Romance scams" typically lead to a fraudster gaining the trust of a victim through romantic overtures and causing them to send their own money to the fraudster, or to receive and send (unwittingly) criminal proceeds at the fraudster's direction.

7. An "advance fee scam" is a type of fraud in which a fraudster asks a victim to pay a fee up front, in advance of receiving any proceeds, money, stock, or warrants, in order for the deal to go through. The advance payment may be described as a fee, tax, commission, or incidental expense that will be repaid later.

8. A "business email compromise scheme" is a type of fraud in which a fraudster

sends email messages that appear to come from a known source making a legitimate request to transfer funds.

9. The affected banks—including TD Bank, Citizens Bank, and Santander Bank—are all financial institutions within the meaning of 18 U.S.C. § 20.

Romance Scam: Victim 1

10. Victim 1 is a 72-year-old woman residing in San Antonio, Texas.

11. Based on interviews with Victim 1 and other evidence I have reviewed as part of this investigation, I am aware that in or about November 2017, Victim 1 received a "friend request" via Facebook from an individual previously unknown to her, who went by the name "Gibson Banks." Victim 1 accepted the friend request, and shortly thereafter, "Banks" privately messaged her. Victim 1 and Banks subsequently began communicating on a regular basis. "Banks" told Victim 1 that he was a soldier in the U.S. Army conducting Special Operations missions across the world and was currently working in Syria. Victim 1 also communicated with "Banks" via text message and believed she was in a romantic relationship with "Banks," despite never meeting him in person or speaking to him on the telephone.

12. "Banks" told Victim 1 that he had come into millions of dollars while working in Iraq, and asked Victim 1 to send him money so that he could access his money overseas. Banks asked Victim 1 to travel to Belgium to retrieve a "consignment box" containing $24 million and promised her part of the funds in return for her effort. In or about January 2018, Victim 1 traveled to Belgium, where she met an unknown man who went by the name "Daniel." Victim 1 brought $10,000 with her, which "Banks" had told her was needed to obtain the "consignment box." "Banks" told Victim 1 they needed more money to obtain the box, and she traveled to various

Western Union locations around Antwerp and Brussels and used her credit cards to withdraw an additional approximately $26,000. Victim 1 gave the funds to "Daniel."

13. After Victim 1 returned to the United States, "Daniel" contacted her and said he needed another $92,000, which Victim 1 wired to "Daniel."

14. "Banks" continued to give Victim 1 excuses for needing more money, including that he purportedly needed funds to purchase special chemicals to remove ink from the currency in the "consignment box," to give to authorities to get those funds out of the country, to cover costs of children who were sick, and to raise money to secure "Banks's" release from a Syrian prison.

15. For example, in or about the fall and winter of 2019, Victim 1 sent $70,000 in cashier's checks to "James," a friend of "Banks," who was purportedly raising money to secure "Banks's" release from prison. During that period, Victim 1 communicated with "James" approximately twice per week.

16. In total, Victim 1 sent more than $720,000 in funds at the direction of "Banks" or his associates.

The TD Bank 7685 Account

17. On or about October 18, 2019, an account in the name of Jacob Emmanuel with an account number ending in 7685 ("the 7685 Account") was opened at a TD Bank branch in Reading, Massachusetts. To open the account, the person purporting to be Jacob Emmanuel presented a South African passport bearing the number A04719653 and showing a date of birth of February 16, 1979. The mailing address used to open this account was recorded as 125 Norfolk Street, Boston, MA 02124.

18. I have queried Customs and Border Protection ("CBP") border crossing databases for information about a Jacob Emmanuel born on February 16, 1979 and using South African passport #A04719653. No information was found, which leads me to believe that the passport used to open the 7685 Account was fake and/or that Jacob Emmanuel did not enter the United States at a designated Port of Entry.

19. TD Bank surveillance images from the opening of the 7685 Account depict a man who appears to be UMEH, walking with a TD Bank employee to the ATM outside the branch, and then using the ATM the day the 7685 Account was opened:

20. TD Bank surveillance images from on or about October 19, 2019—the day after the 7685 Account was opened—show a co-conspirator, MIKE OZIEGBE AMIEGBE, depositing a $10,000 cashier's check from Victim 1 and made out to Jacob Emmanuel into the 7685 Account.[1]

[1] In March 2021, AMIEGBE was charged by complaint in the United States District Court for the District of Massachusetts on one count of conspiracy to commit mail fraud, in violation of 18 U.S.C. § 1349. *See United States v. Amiegbe*, No. 21-cr-10339-IT-DLC. On February 16,

21. The $10,000 cashier's check deposited into the 7685 Account was promptly withdrawn in the form of a $7,600 cash withdrawal on or about October 24, 2019 and a $2,350 cash withdrawal on or about October 25, 2019. TD Bank surveillance images from October 24, 2019 appear to depict UMEH making the $7,600 withdrawal and handing the teller a passport:

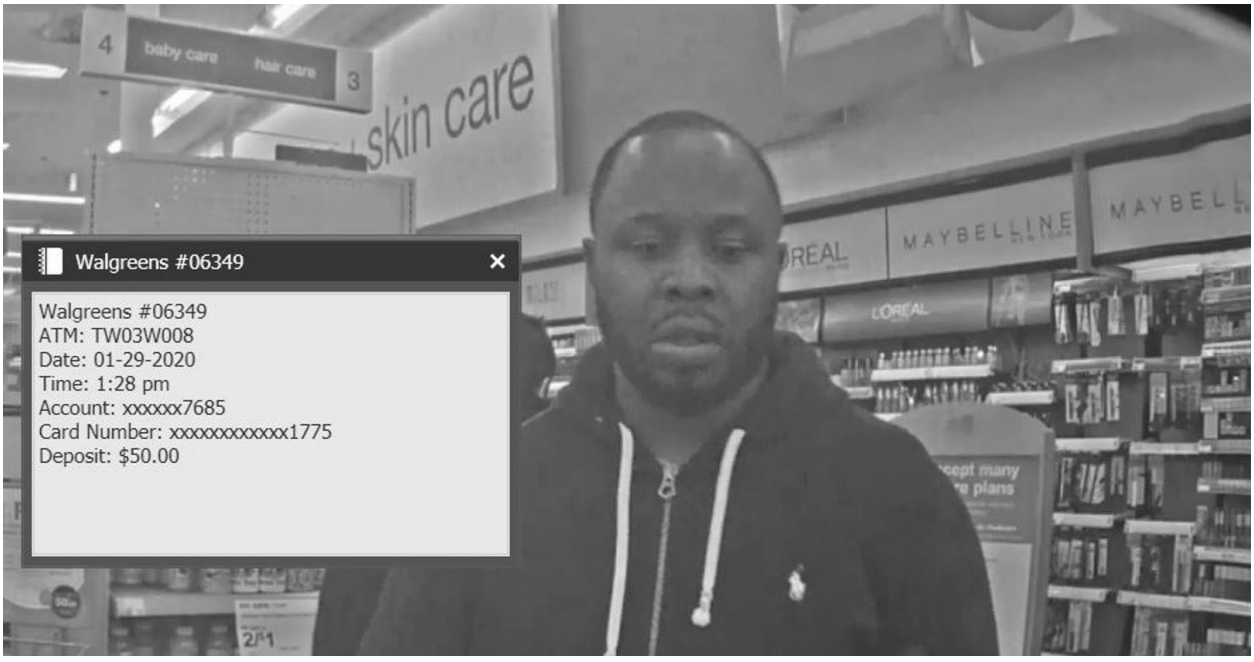
22. TD Bank surveillance images from October 25, 2019 appear to depict UMEH making the $2,350 withdrawal and handing the teller a passport:

2022, AMIEGBE pleaded guilty to an information charging conspiracy to commit mail fraud, in violation of 18 U.S.C. § 1349, for his conduct described herein, among other things. His sentencing is pending.

23. On or about October 29, 2019, TD Bank surveillance images show AMIEGBE depositing a $14,000 cashier's check from Victim 1 and made out to Jacob Emmanuel into the 7685 Account:

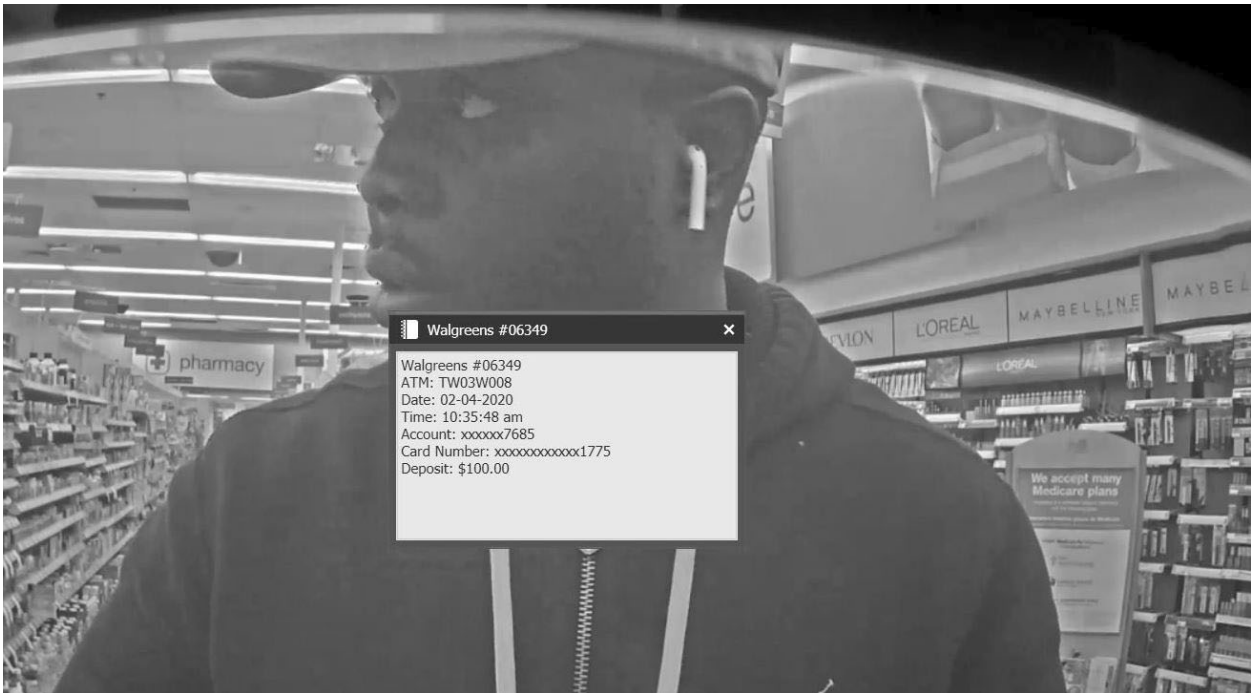
24. The $14,000 cashier's check deposited into the 7685 Account was promptly withdrawn in the form of a $7,780 cash withdrawal on or about November 2, 2019 and a $6,180 cash withdrawal on or about November 4, 2019. No surveillance exists for the November 2, 2019 withdrawal, but TD Bank surveillance of the November 4, 2019 withdrawal appears to depict UMEH making the $6,180 withdrawal and handing the teller a passport:

25. TD Bank surveillance images from on or about January 29, 2020 for an ATM located inside a Walgreens store located in Dorchester, Massachusetts appear to depict UMEH depositing $50.00 into the 7685 Account. In that video, UMEH is wearing what appears to be a navy zip-up "hoodie" sweatshirt with a yellow "Polo" logo:



26. TD Bank surveillance images from on or about February 4, 2020 for an ATM located inside the Walgreens store in Dorchester, Massachusetts appear to depict UMEH

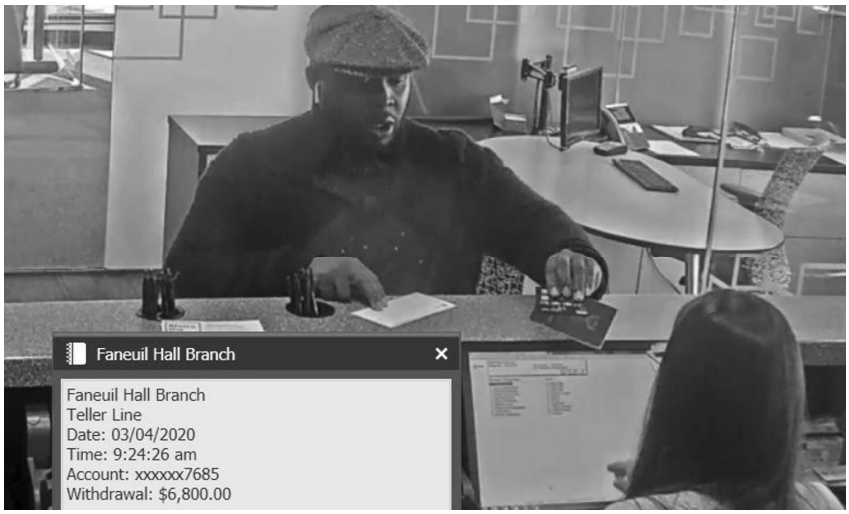
depositing $100.00 into the 7685 Account. In that video, UMEH is wearing what appears to be the same navy "Polo" sweatshirt.



27. TD Bank surveillance images from on or about February 14, 2020 appear to depict UMEH depositing $40.00 into the 7685 Account. In that video, UMEH is wearing what appears to be the same navy "Polo" sweatshirt:

28. On or about March 3, 2020, the 7685 Account received a wire transfer from an individual in Portugal in the amount of $12,820.59.[2] Those funds were promptly withdrawn in the form of a $6,800 cash withdrawal on or about March 4, 2020 and a $5,600 cash withdrawal on or about March 5, 2020. TD Bank surveillance images from March 4, 2020 depict a man who appears to be UMEH making the $6,800 withdrawal and handing the teller a passport. In the video, UMEH appears to be wearing a flat gray "newsboy" style hat:

[2] Because this wire came from an individual located outside the United States, I have not been able to interview the individual to confirm whether he or she was a victim of a scam, but given the uses to which UMEH and others have put the 7685 Account, there is probable cause to believe that the approximately $12,800 was criminally derived.



29. TD Bank surveillance images from on or about March 5, 2020 depict a man who appears to be UMEH making the $5,600 withdrawal and handing the teller a passport. In the video, UMEH appears to be wearing the same flat gray "newsboy" style hat along with a dark, button-down shirt with polka dots:

30. On or about April 27, 2020, the 7685 Account received a deposit for a $25,000 cashier's check.[3] No surveillance exists for this deposit. These funds were promptly withdrawn

[3] I have not yet been able to interview the individual on whose account this cashier's check was drawn. However, from my experience and information provided by other law enforcement officers, I know that in these types of romance scam and counterfeit check cases, cashier's checks

in the form of a $7,900 cash withdrawal on or about April 29, 2020, a $7,000 cash withdrawal on or about April 30, 2020, a $4,000 cash withdrawal on or about May 1, 2020, and a $2,300 cash withdrawal also on or about May 1, 2020.

31. TD Bank surveillance images from the April 29, 2020 cash withdrawal depict a man of the same build as UMEH, but the face is difficult to see. TD Bank surveillance images from a drive-up ATM from the April 30, 2020 cash withdrawal depict a man who appears to be UMEH putting a passport into the bank's vacuum tube system. In the video, UMEH appears to be wearing the same dark, button-down shirt with polka dots as he was wearing in the March 5, 2020 surveillance images. He is driving an Acura SUV with Massachusetts license plate 2SS 387.[4]

often come either from (a) victims or (b) victim funds withdrawn from another alias bank account, which are then deposited into a different account to conceal the source and nature of the funds.

[4] Through law enforcement checks, I know that this vehicle is not registered to UMEH. The relationship between UMEH, the Acura SUV, and the registered owner is unknown at this time.

32. TD Bank surveillance images from a separate, $800 cash withdrawal transaction on or about April 30, 2020 depict a man of the same build as UMEH withdrawing money from an ATM. The man is wearing a face covering, but has the same dark, button-down polka dot shirt that UMEH wore in other surveillance video from the 7685 Account, including the $7,000 cash withdrawal that same day.

33. TD Bank surveillance images from a drive-up ATM on or about May 1, 2020 depict a man wearing a face mask and driving the same Acura SUV with Massachusetts license plate 2SS 387 as in the April 30, 2020 surveillance images. TD Bank surveillance images from a drive-up ATM for a second transaction on or about May 1, 2020 depict a man wearing a face mask. The type of vehicle he is driving and license plate number are not visible in the images, although it appears to be a silver SUV similar to the Acura with Massachusetts license plate 2SS 387.

34. Another individual, who investigators have identified as KOFI OSEI, appears on TD Bank surveillance using the 7685 Account on four occasions in or about January 2020.[5]

35. Additionally, between on or about May 7, 2020 and on or about May 22, 2020, multiple deposits from the Massachusetts Department of Unemployment Assurance for pandemic unemployment assistance totaling approximately $25,355 in the names of multiple individuals (other than "Jacob Emmanuel," UMEH, AMIEGBE, or OSEI) were deposited into the 7685 Account.

Counterfeit Check Scheme: Victim 2

36. Victim 2 is a California-based cash advance company offering funds to individuals awaiting court settlements.

37. In or about October 2018, a lawyer ("Lawyer 1") approached Victim 2 on behalf of his client, "Stephen Beuchaws," about providing funding to "Beuchaws," who was purportedly awaiting a wrongful termination settlement from his former employer, Pfizer Inc.

38. "Beuchaws" had provided Lawyer 1 with documents, including documents purportedly on Pfizer letterhead, supporting his wrongful termination claim. "Beuchaws" also provided Lawyer 1 with a cashier's check, purportedly from HSBC Bank and drawn on Pfizer's account, payable to Lawyer 1 for $472,284.

39. As a result of these representations, at "Beuchaws" direction, Victim 2 wired a total of $78,300 to a TD Bank account in the name of Kelvin Thomas with an account number ending

[5] In February 2021, OSEI was indicted in the United States District Court for the District of Massachusetts on charges of making a false statement to a bank, in violation of 18 U.S.C. § 1014, wire fraud, in violation of 18 U.S.C. § 1343, and money laundering, in violation of 18 U.S.C. § 1956, in connection with his role in an online romance scam. *See United States v. Osei*, No. 21-cr-10064-IT. A Rule 11 hearing has been scheduled for August 2, 2022.

in 6073 ("the 6073 Account"). Specifically, Victim 2 wired $50,000 on or about November 26, 2018; $8,300 on or about December 7, 2018; and $20,000 on or about December 28, 2018.

The TD Bank 6073 Account

40. On or about November 21, 2018, an individual purporting to be Kelvin Thomas opened the 6073 Account at a TD Bank branch in Boston, Massachusetts. "Thomas" presented TD Bank with a South African passport bearing the number I9402440 and showing a date of birth of January 11, 1985. The mailing address used to open this account was recorded as 12 East Street, Dorchester, Massachusetts 02122. Law enforcement databases indicate that, between in or about December 2014 through in or about September 2016, UMEH resided at 12 East Street, Apt. 1, Dorchester, Massachusetts 02122.

41. I have queried Customs and Border Protection ("CBP") border crossing databases for information about a Kelvin Thomas born on January 11, 1985 and using South African passport #I9402440. No information was found, which leads me to believe that the passport is fake and/or that Kelvin Thomas did not enter the United States at a designated Port of Entry.

42. As noted above, Victim 2 wired $50,000 to the 6073 Account on or about November 26, 2018. TD Bank surveillance images depict a man who appears to be UMEH withdrawing $8,000 from the 6073 Account two days later, on or about November 28, 2018. In the image below, UMEH appears to be wearing the same flat, gray "newsboy" hat that he wore when accessing the 7685 Account (in the name of Jacob Emmanuel) on or about March 4, 2020.

Text Messages with UMEH

43. In connection with the related investigation of KOFI OSEI, on or about February 25, 2021, investigators executed search warrants at OSEI's residence and on his car. *See In the Matter of the Search of 95 Bridle Path Circle, #930, Randolph, Massachusetts*, No. 21-mj-1043-DLC*; In the Matter of the Search of 95 Bridle Path Circle, #930, Randolph, Massachusetts, Second Bedroom*, No. 21-mj-1046-DLC; *In the Matter of the Search of 2014 Lexus IS350 F-Sport, VIN JTHCE1D23E5003343, with Temporary Plate 02536U4*, No. 21-mj-1047-DLC. Evidence seized during this search included digital data extracted from phones found in OSEI's residence, including an Apple iPhone Red SE (2nd generation) ("OSEI's Phone").

44. In connection with the related investigation of MIKE OZIEGBE AMIEGBE, on or about March 25, 2021, investigators executed a search warrant at AMIEGBE's residence. *See In the Matter of the Search of 41 Supple Road, Apt. 1, Dorchester, Massachusetts*, No. 21-mj-1192-

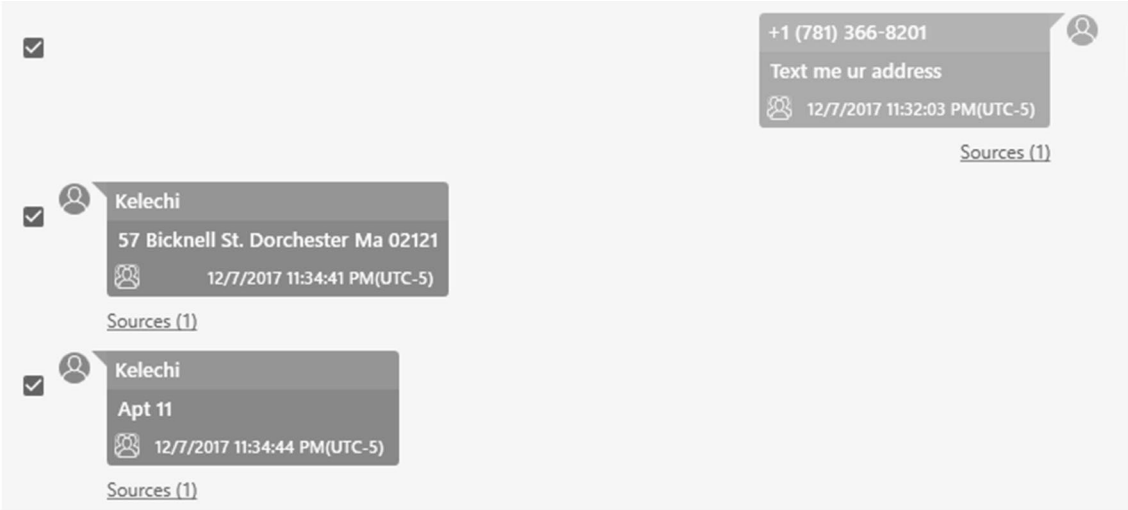
DLC. Evidence seized during this search included digital data extracted from phones found in Mike AMIEGBE's bedroom, specifically an Apple iPhone 11 Pro Max ("AMIEGBE's Phone").

45. One of the contacts listed in both OSEI's Phone and AMIEGBE's Phone was 617-870-8725. According to Verizon records, 617-870-8725 has been subscribed to Kelechi UMEH of 57 Bicknell Street, Dorchester, Massachusetts since at least December 27, 2018. OSEI saved the contact with the number 617-870-8725 as "Kelechi." AMIEGBE saved the contact with the number 617-870-8725 as "Shop New."

46. Several videos saved to AMIEGBE's Phone that were sent to AMIEGBE from the 617-870-8725 number appear to include footage of UMEH. For example, below is a screen capture from one of the videos. An announcer can be heard in the background of this video asking the UMEH family to come to the center of the room to cut a birthday cake.

47. OSEI also exchanged messages with "Kelechi" at the 617-870-8725 number via WhatsApp. For example:

a. On or about December 7, 2017, OSEI sent a message to "Kelechi" asking for his address, to which "Kelechi" responded, "57 Bicknell St. Dorchester Ma 02121.



According to law enforcement databases, UMEH resided at 57 Bicknell Street #11, Dorchester, MA from on or about May 2018 through on or about December 2021.

b. On or about February 22, 2018, "Kelechi" sent a message to OSEI that read: "125 Norfolk Street, Dorchester, MA." On or about April 18, 2018, "Kelechi" sent the same message to OSEI: "125 Norfolk st. Dorchester Ma 02124." He repeated the message on or about April 16, 2019: "125 Norfolk st. Dorchester ma 02124." On or about January 17, 2020, OSEI sent a message to "Kelechi" asking for a "Zip code," to which "Kelechi" replied, "02124." As noted above, the 125 Norfolk St., Dorchester, Massachusetts 02124 address was used in opening the 7685 Account in the name of Jacob Emmanuel. Bank records show that this address (125 Norfolk Street,

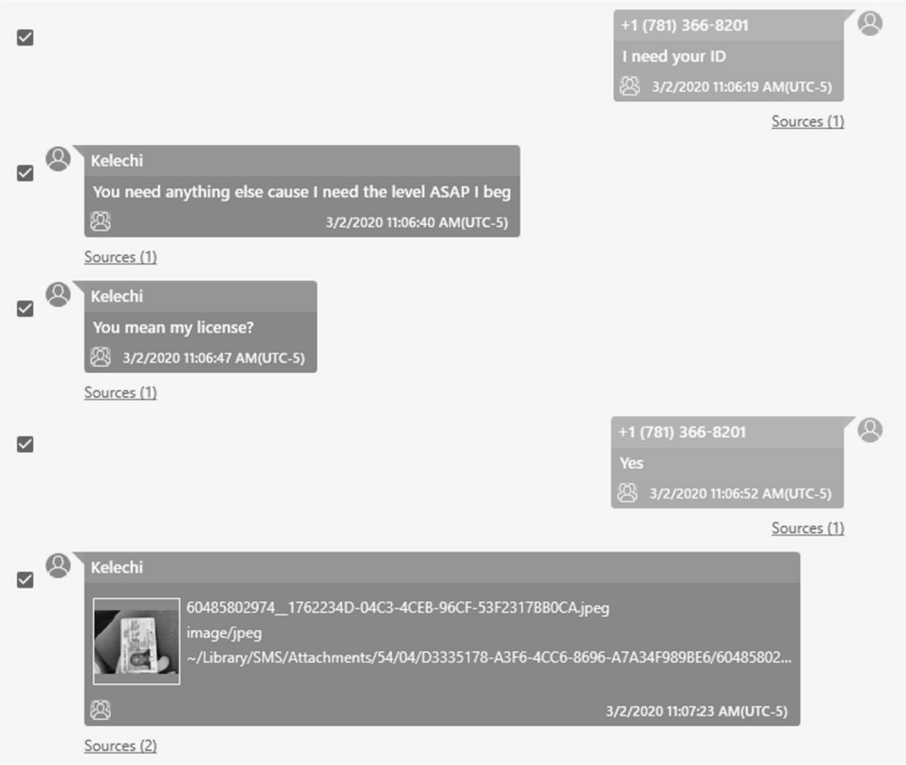
Dorchester, MA) was also used to open additional bank accounts in the names of Jacob Emmanuel, as well as bank accounts in the names of Kelvin Thomas, Brian Morgan, Paul Douglas, Isiah John/John Isiah, and James Emmanuel, each of which was opened using a fake passport.

c. On or about April 4, 2019, OSEI sent a message to "Kelechi" with the name "James niro." I am aware that "James Niro" or "Niro James" was an alias used by another co-conspirator, FRANCIS OKAFOR, to open bank accounts for receiving victim funds.[6]

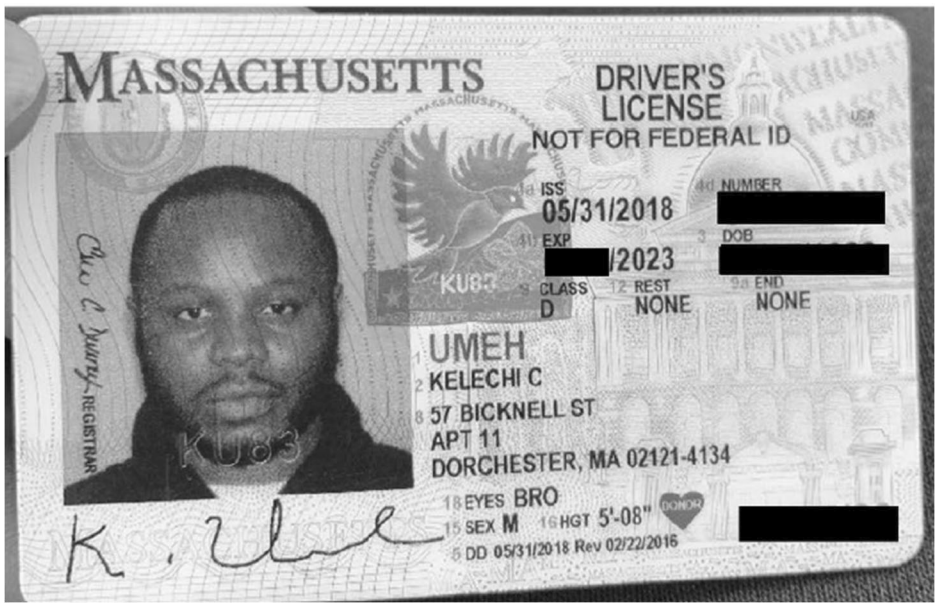
d. On or about August 31, 2019, "Kelechi" sent a message to OSEI that read as follows: "I need all of them without online access for wire from 100K to 400k," and then listed "VENUS BANK. STERLING BANK. ORACLE BANK. FIRST CITIZENS BANK. MINYANINK BANK." "Kelechi" ended the message with, "For Wire Loading. USA to USA. 100k to 400k." "Kelechi" then asked OSEI, "U fit run this?" and "One of my guy for dubia need this urgently."

e. On or about March 20, 2020, OSEI sent a message to "Kelechi" asking for a copy of his identification in connection with the purchase of a car at auction.

[6] In August 2021, OKAFOR was charged by complaint in the United States District Court for the District of Massachusetts with one count of conspiracy to commit bank and wire fraud, in violation of 18 U.S.C. § 1349. *See United States v. Okafor*, No. 22-cr-10095-DPW. On April 4, 2022, OKAFOR agreed to plead guilty to an information charging conspiracy to commit bank fraud, in violation of 18 U.S.C. § 1349, for the conduct described herein, among other things. His plea hearing is scheduled for August 30, 2022.



The license "Kelechi" sent back to OSEI depicts UMEH:[7]



[7] I have redacted the license number and date of birth.

The man depicted in the MA driver's license appears to be the same person I viewed in videos saved to AMIEGBE's phone, under the contact "Shop New," and the man I recognize from bank surveillance images from the 7685 Account in the name of Jacob Emmanuel and the 6073 Account in the name of Kelvin Thomas.

Additional Accounts

48. In addition to the 7685 Account and 6073 Account described above, the investigation to date has linked UMEH with the following assumed names and accounts, all opened with passports that appear to be fake:

Alias	Bank	Account (Last 4)	Account Address	Account Telephone	Account Email
Jacob Emmanuel	TD Bank	7685	125 Norfolk St. Boston, MA 02124		Autoshop147@mail.com
James Emmanuel	TD Bank	6445	125 Norfolk St. Boston, MA 02124		Emmacarshop147@gmail.com
Kelvin Thomas	TD Bank	6073 0075	12 East St. Dorchester, MA 02124		Workbox014701@gmail.com
Kelvin Thomas	Citizens Bank	7346 1669	125 Norfolk St. Boston, MA 02124		
John Isiah	Santander Bank	7646 0711	125 Norfolk St. Boston, MA 02124	404-547-2515	Workbox014701@gmail.com
John Isiah	Santander Bank	0210	35 Newport St., Apt. 2 Dorchester, MA 02125	404-547-2515	kglake@yahoo.com
Brian Morgan	Citizens Bank	3171 3664	125 Norfolk St. Boston, MA 02124		
Paul Douglas	TD Bank	5706	70 Readville St., Apt. C Hyde Park, MA 02136		Workbox0147@gmail.com

THE TARGET PREMISES CONTAIN EVIDENCE, FRUITS, AND INSTRUMENTALITIES OF THE TARGET OFFENSES

49. For the reasons stated below, there is probable cause to believe that the TARGET PREMISES contain fruits, evidence, and instrumentalities of the TARGET OFFENSES, as described in Attachment B to the proposed warrant.

50. From my training, experience, and information provided to me by other agents, I am aware that individuals frequently use computers to create and store records of their actions by communicating about them through e-mail, instant messages, and updates to online social-networking websites; drafting letters; keeping their calendars; arranging for travel; storing pictures; researching topics of interest; buying and selling items online; and accessing their bank, financial, investment, utility, and other accounts online.

51. Based on my training, experience, and information provided by other law enforcement officers, I know that many cell phones (which are included in Attachment B's definition of "hardware") can now function essentially as small computers. Phones have capabilities that include serving as a wireless telephone to make audio calls, digital camera, portable media player, GPS navigation device, sending and receiving text messages and emails, and storing a range and amount of electronic data. Examining data stored on devices of this type can uncover, among other things, evidence of communications and evidence of communications and evidence that reveals or suggests who possessed or used the device.

52. I am aware of a report from the United States Census Bureau that shows that in 2018, among all households nationally, 92 percent had a computer, which includes smartphones, and 85 percent had a broadband Internet subscription. Specifically, in 2018, the use of smartphone

ownership surpassed all other computing devices. 84 percent of households had a smartphone and 63 percent of households had a tablet, and 78 percent of households had a desktop or laptop computer. Further, according to the Pew Research Center, as of 2021, 97 percent of adult Americans own a cellphone, and 85 percent own a cellphone with significant computing capability (a "smartphone"). The percentage of adults that own a smartphone is even higher among younger demographic groups: 96 percent of 18-29 year olds, 95 percent of 30-49 year olds, and 83 percent of 50-64 year olds owned smartphones in 2021.

53. In my training and experience and information provided by other law enforcement officers, I know that in romance and business email compromise schemes, co-conspirators often communicate with each other about the scheme. These communications often occur through encrypted messaging applications such as WhatsApp, over text message, or by email. For example, co-conspirators who open bank accounts using aliases often share account information with co-conspirators communicating with victims so the latter can tell the victims where to send money. Similarly, co-conspirators who communicate with victims often tell co-conspirators who open fraudulent bank accounts when to expect a deposit so that the funds can be quickly withdrawn and distributed among co-conspirators. Indeed, the timing of deposits and withdrawals described above suggests close communication between co-conspirators in that UMEH generally withdrew funds within days of a victim deposit. Additionally, co-conspirators who share access to fraudulent accounts, such as UMEH, AMIEGBE, and OSEI, often communicate with each other regarding information needed to access the accounts, such as information to verify an address.

54. As described above, UMEH exchanged WhatsApp messages with OSEI concerning the 125 Norfolk Street, Dorchester, Massachusetts address, an address used to open several of the

bank accounts described herein, including the 7685 Account at TD Bank in the name of Jacob Emmanuel. UMEH also exchanged messages with OSEI concerning "James Niro," an alias used by co-conspirator OKAFOR to open bank accounts for receiving victim funds.

55. In my training and experience and information provided by other law enforcement officers, I know that in romance and business email compromise schemes, co-conspirators often check account balances through online banking applications. For example, records from TD Bank reflect that the 7685 Account in the name of Jacob Emmanuel was accessed 13 times via cell phone and computer between on or about October 18, 2019 and on or about May 31, 2020. Records from TD Bank reflect that the 6073 Account in the name of Kelvin Thomas was accessed 3 times via cell phone and computer in or about November and December 2018.

56. Although more than two years have passed since the accounts identified above have been active, I believe evidence of the TARGET OFFENSES will nevertheless be found in the TARGET PREMISES, specifically on UMEH's cell phone. In my training and experience, individuals tend to "backup" their phones to the "cloud," such that the information is accessible despite the passage of time and even if UMEH replaced his phone in the intervening period. Additionally, in my experience, individuals tend to keep communications on their cell phones going back years. Indeed, when investigators searched the OSEI phone in 2021, they found WhatsApp messages from "Kelechi" (whom I believe to be UMEH) dating back to 2017. Similarly, when investigators searched the AMIEGBE phone in 2021, they found WhatsApp messages from the "Shop New" contact that I believe to be UMEH dating back to 2019.

57. I am aware that UMEH has booked a flight from Boston to Los Angeles for July 22, 2022 (Jet Blue #287, departing at 7 a.m. EDT and arriving at 10:25 a.m. PDT), with a return

flight scheduled for July 25, 2022 (Jet Blue #988, departing at 1137 p.m. PDT on July 25 and arriving at 7:50 a.m. EDT on July 26). In my experience, individuals who are traveling by plane tend to keep their cell phone on their person. Additionally, I conducted surveillance of the boarding area of Jet Blue Flight #287 on the morning of July 22, 2022, and I saw a man I recognize to be UMEH board the plane holding what appeared to be a cell phone in his hand. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device.

58. Based on my knowledge, training, experience, and information provided to me by other agents, I know that computer files or remnants of such files can be recovered months or years after they have been written, downloaded, saved, deleted, or viewed locally or over the Internet. This is true because:

a. Electronic files that have been downloaded to a storage medium can be stored for years at little or no cost. Furthermore, when users replace their computers, they can easily transfer the data from their old computer to their new computer.

b. Even after files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data, which might not occur for long periods of time. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in

particular, computers' internal hard drives—contain electronic evidence of how the computer has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. It is technically possible to delete this information, but computer users typically do not erase or delete this evidence because special software is typically required for that task.

d. Similarly, files that have been viewed over the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache." The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are overwritten only as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

e. Data on a storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record

information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

f. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of

computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

g. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

h. The process of identifying the exact files, blocks, registry entries, logs, or

other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

i. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

59. Based on my knowledge and training and the experience of other agents with whom I have spoken, I am aware that in order to completely and accurately retrieve data maintained in computer hardware, computer software or storage media, to ensure the accuracy and completeness of such data, and to prevent the loss of the data either from accidental or programmed destruction, it is often necessary that computer hardware, computer software, and storage media ("computer equipment") be seized and subsequently processed by a computer specialist in a laboratory setting rather than in the location where it is seized. This is true because of:

j. The volume of evidence — storage media such as hard disks, flash drives, CDs, and DVDs can store the equivalent of thousands or, in some instances,

millions of pages of information. Additionally, a user may seek to conceal evidence by storing it in random order or with deceptive file names. Searching authorities may need to examine all the stored data to determine which particular files are evidence, fruits, or instrumentalities of criminal activity. This process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this analysis on-site.

k. Technical requirements — analyzing computer hardware, computer software or storage media for criminal evidence is a highly technical process requiring expertise and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications. Thus, it is difficult to know, before the search, which expert possesses sufficient specialized skill to best analyze the system and its data. Furthermore, data analysis protocols are exacting procedures, designed to protect the integrity of the evidence and to recover even "hidden," deleted, compressed, or encrypted files. Many commercial computer software programs also save data in unique formats that are not conducive to standard data searches. Additionally, computer evidence is extremely vulnerable to tampering or destruction, both from external sources and destructive code imbedded in the system as a "booby trap."

Consequently, law enforcement agents may either copy the data at the premises to be searched or seize the computer equipment for subsequent processing elsewhere.

60. The premises may contain computer equipment whose use in the crime(s) or storage

of the things described in this warrant is impractical to determine at the scene. Computer equipment and data can be disguised, mislabeled, or used without the owner's knowledge. In addition, technical, time, safety, or other constraints can prevent definitive determination of their ownership at the premises during the execution of this warrant. If the things described in Attachment B are of the type that might be found on any of the computer equipment, this application seeks permission to search and seize it onsite or off-site in order to determine their true use or contents, regardless of how the contents or ownership appear or are described by people at the scene of the search.

61. This warrant authorizes a review of electronic storage media seized, electronically stored information, communications, other records and information seized, copied or disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized, copied, or disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

UNLOCKING A DEVICE USING BIOMETRIC FEATURES

62. I know from my training and experience, as well as from information found in publicly available materials, that some models of cellphones made by Apple, Samsung, and other manufacturers, offer their users the ability to unlock a device via the use of a fingerprint or through facial recognition, in lieu of a numeric or alphanumeric passcode or password.

63. For example, on the Apple devices that have this feature, the fingerprint unlocking feature is called Touch ID. If a user enables Touch ID on a given Apple device, he or she can register up to 5 fingerprints that can be used to unlock that device. The user can then use any of the registered fingerprints to unlock the device by pressing the relevant finger(s) to the device's Touch ID sensor. In some circumstances, a fingerprint cannot be used to unlock a device that has Touch ID enabled, and a passcode must be used instead, such as: (1) when more than 48 hours has passed since the last time the device was unlocked and (2) when the device has not been unlocked via Touch ID in 8 hours and the passcode or password has not been entered in the last 6 days. Thus, in the event law enforcement encounters a locked Apple device, the opportunity to unlock the device via Touch ID exists only for a short time. Touch ID also will not work to unlock the device if (1) the device has been turned off or restarted; (2) the device has received a remote lock command; or (3) five unsuccessful attempts to unlock the device via Touch ID are made. I am aware that Android devices often employ a similar feature for fingerprint access.

64. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face. I am aware that Apple devices often employ a similar facial-recognition feature.

65. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

66. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents.

67. The passcode(s) that would unlock UMEH's devices are not currently known to law enforcement. Thus, it may be useful to press the finger(s) of UMEH to the device's fingerprint sensor or to hold the device up to his face in an attempt to unlock the device for the purpose of executing the search authorized by this warrant. The government may not otherwise be able to access the data contained on those devices for the purpose of executing the search authorized by this warrant.

68. For these reasons, I request that the Court authorize law enforcement to press the fingers (including thumbs) of UMEH to the sensor of any cell phone or electronic device on his

person or place them in front of his face for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

CONCLUSION

69. Based on the information described above, there is probable cause to believe that that UMEH has violated 18 U.S.C. § 1349.

70. Based on the information described above, there is also probable cause to believe that evidence, fruits, and instrumentalities of the TARGET OFFENSES, as described in Attachment B to the proposed warrants to search his person, are contained within the TARGET PREMISES described in Attachment A to the proposed warrants.

Sworn to under the pains and penalties of perjury,

DLC

Aaron Lindaman

Aaron Lindaman
Special Agent
Homeland Security Investigations

Subscribed and sworn to before me by telephone on July 22, 2022

Hon. Donald L. Cabell
United States Magistrate Judge